

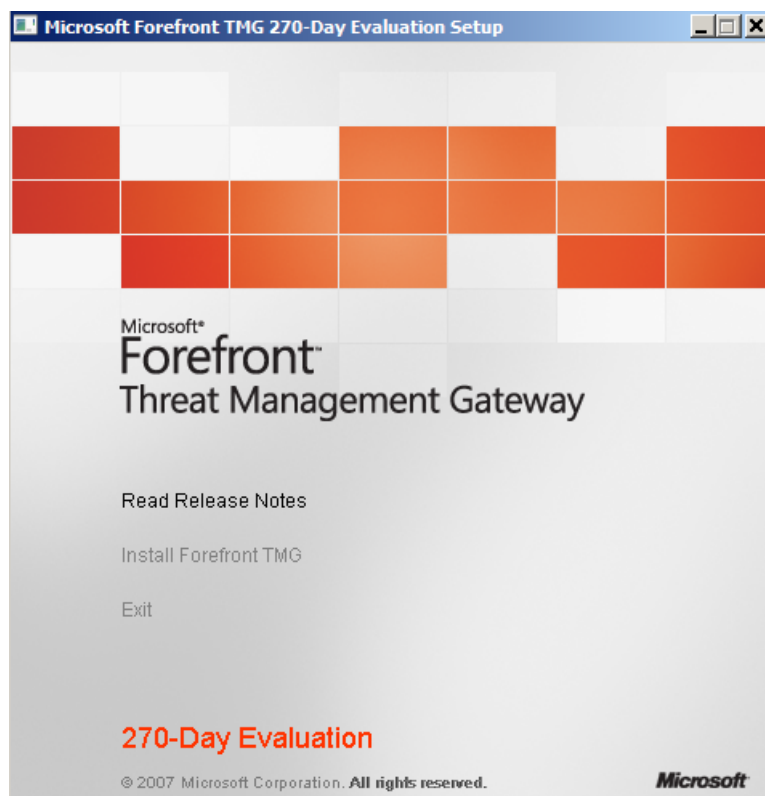
## Microsoft Forefront TMG – Erster Ueberblick

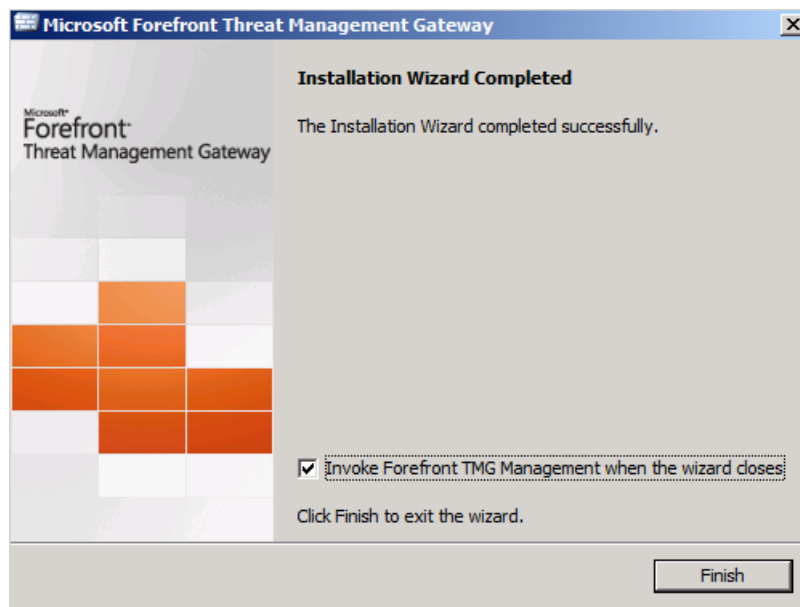
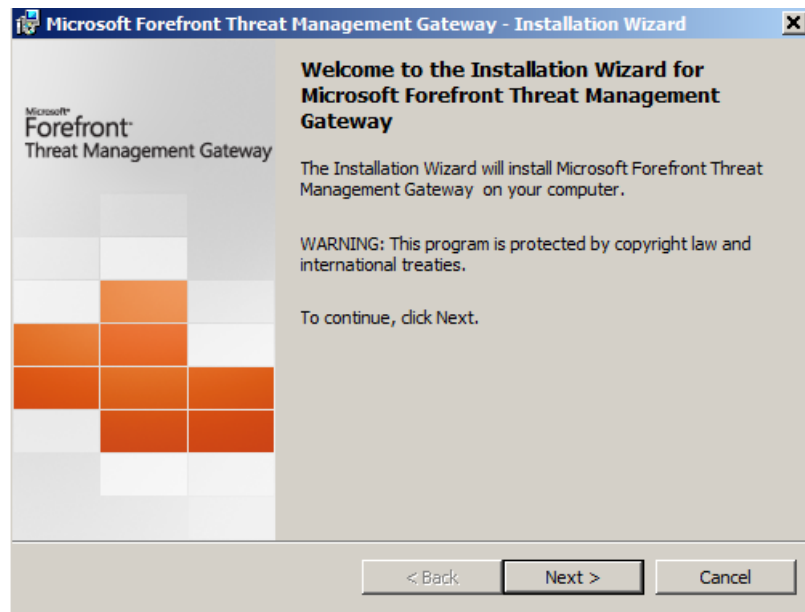
Es folgt ein Ueberblick ueber das Microsoft Forefront TMG Produkt in der Beta Phase. Aus Zeitgruenden folgt als erstes nur ein Ueberblick ueber die wichtigsten Neuerungen in Form von Screenshots mit wenig Erklaerungen. Detaillierte Informationen wird es in Zukunft auf meinem Blog und auf Dieters [www.msisafaq.de](http://www.msisafaq.de) Seite geben.

Der Test erfolgte auf einem Hyper-V Server. Die VM ist ein Windows Server 2008 64 Bit System auf Englisch - ES GEHT ENDLICH.

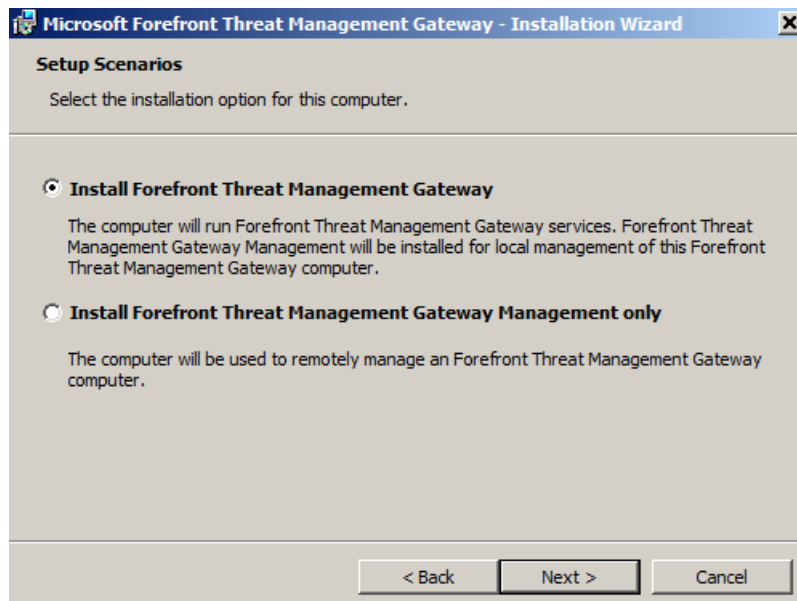
Immer daran denken, es handelt sich um eine Beta. Der Funktionsumfang hat sich gegenueber meinem ersten Beta Zugang vor knapp einem Jahr nicht wesentlich geaendert.

### Installation

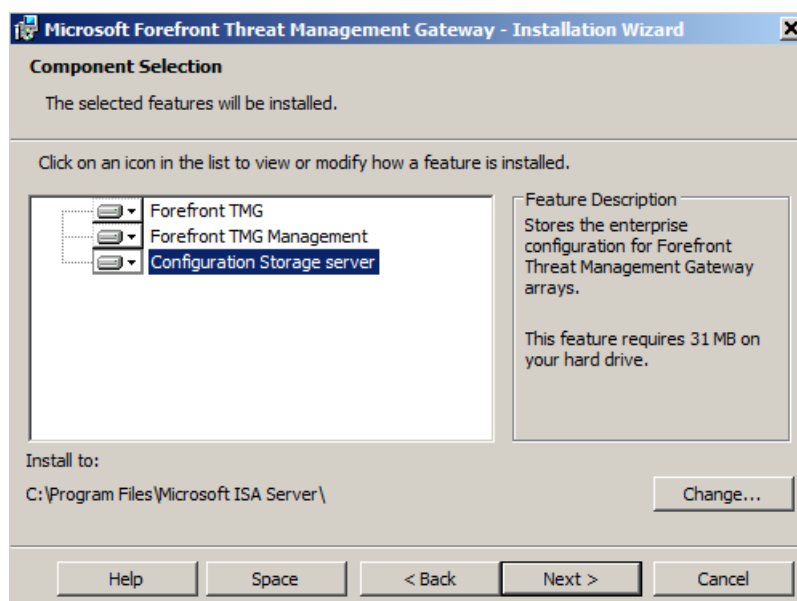




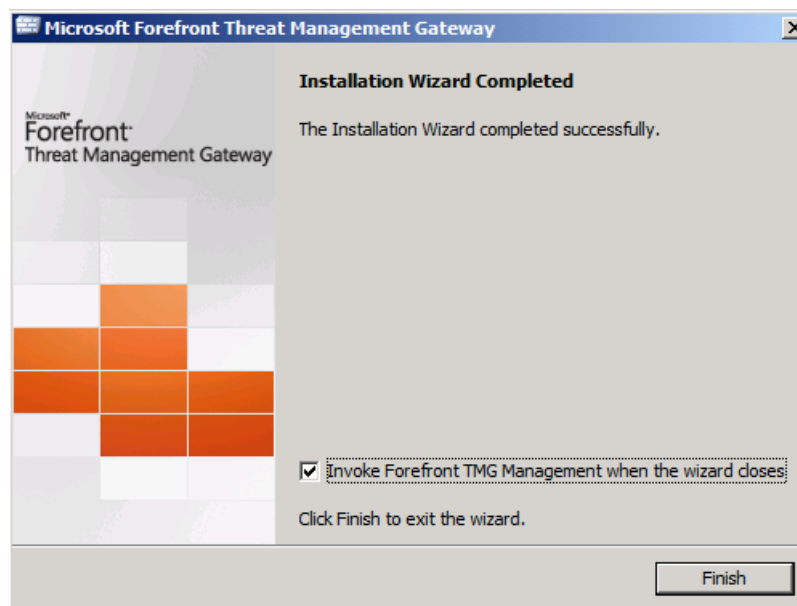
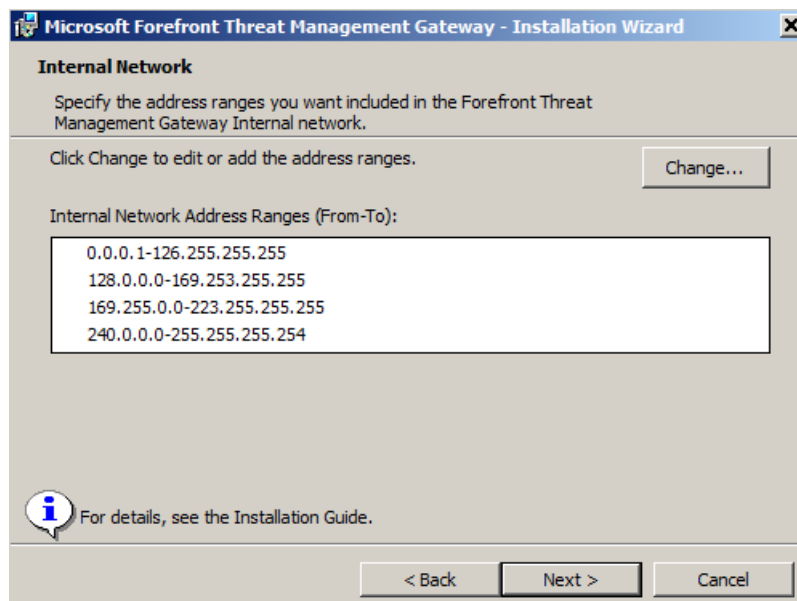
Installation des TMG

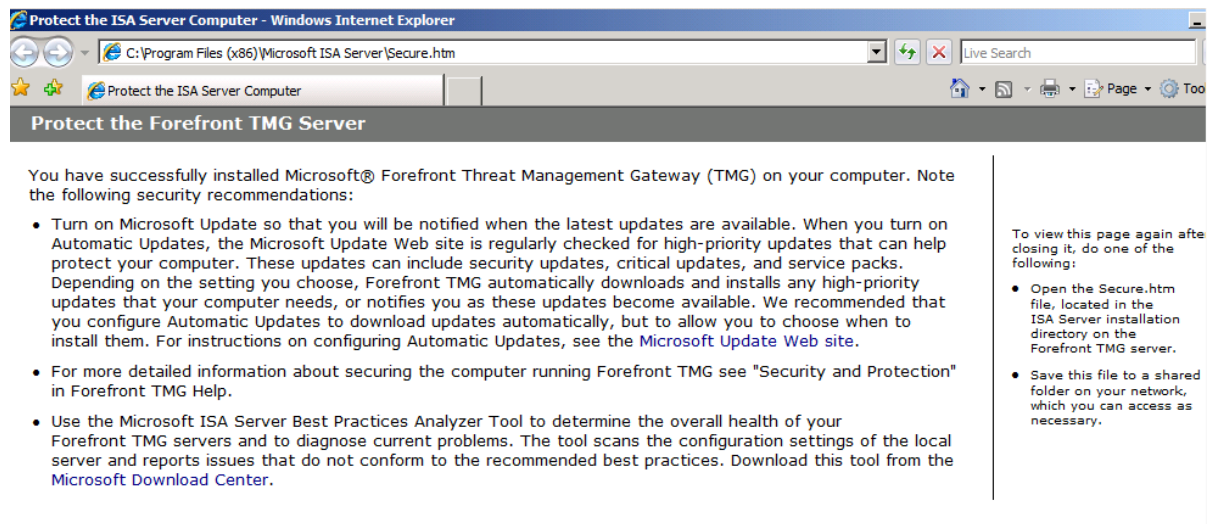


## Auswahl der Komponenten

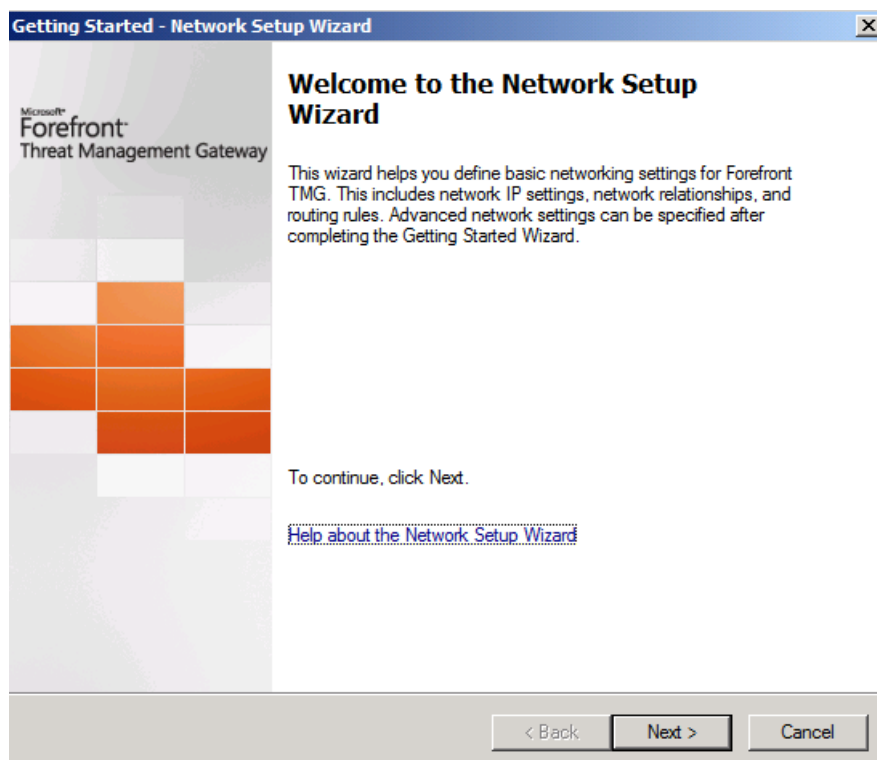
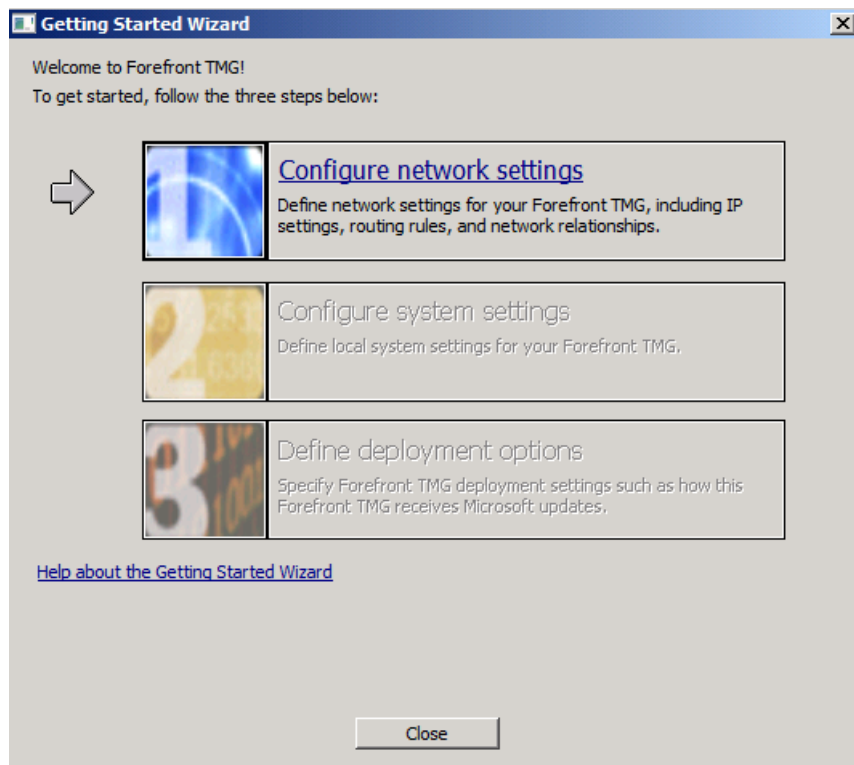


## Auswahl der Netzwerke





Neu: Ein grundlegender Setup Wizard

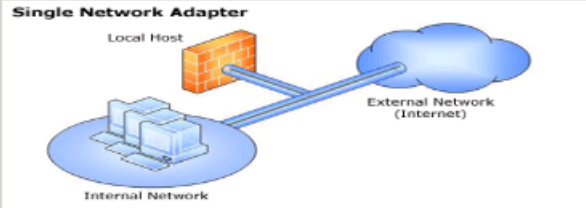


**Getting Started - Network Setup Wizard**

**Network Template Selection**  
Select the network template that best fits your network topology.

☐ Edge firewall  
☐ 3-Leg perimeter  
☐ Back firewall  
☒ Single NIC

**Single Network Adapter**



The diagram illustrates the 'Single Network Adapter' topology. It shows a 'Local Host' (represented by a brick wall) connected to an 'Internal Network' (represented by a blue cloud with server icons). The 'Local Host' is also connected to an 'External Network (Internet)' (represented by a blue cloud). The connection between the 'Local Host' and the 'Internal Network' is labeled 'Single Network Adapter'.

In this topology, Forefront TMG is connected with a single network adapter to the Internal network or the Perimeter network. In this topology, Forefront TMG can protect internal clients from Web and e-mail threats, provide remote access to internal applications, and accelerate access to the Internet.

< Back   Next >   Cancel


**Getting Started - Network Setup Wizard**

**Local Area Network (LAN) Settings**  
Define the settings for the network adapter connected to your LAN.

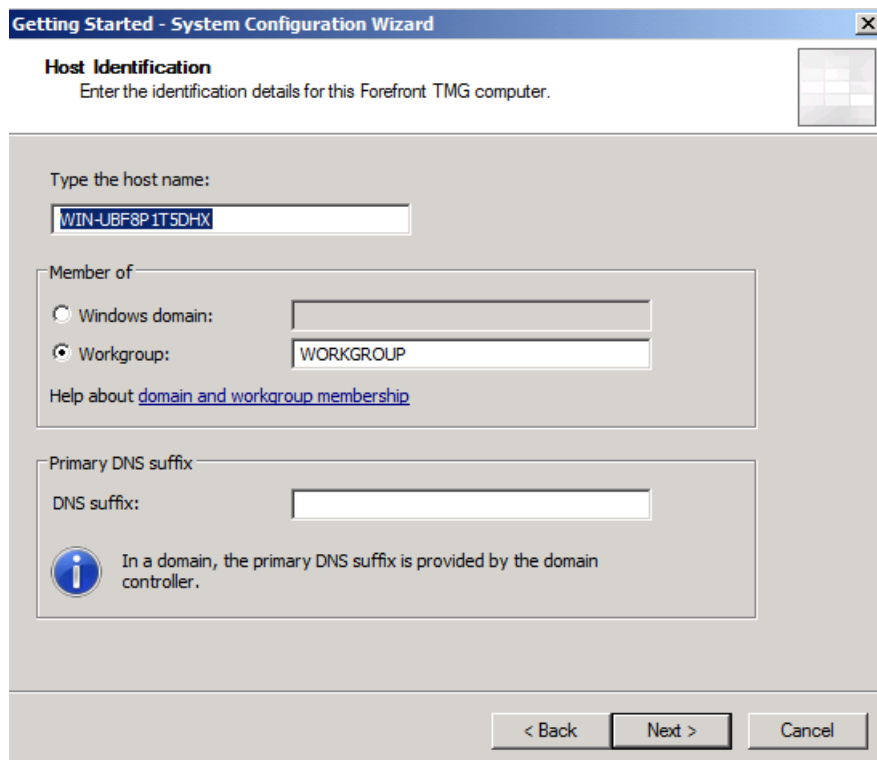
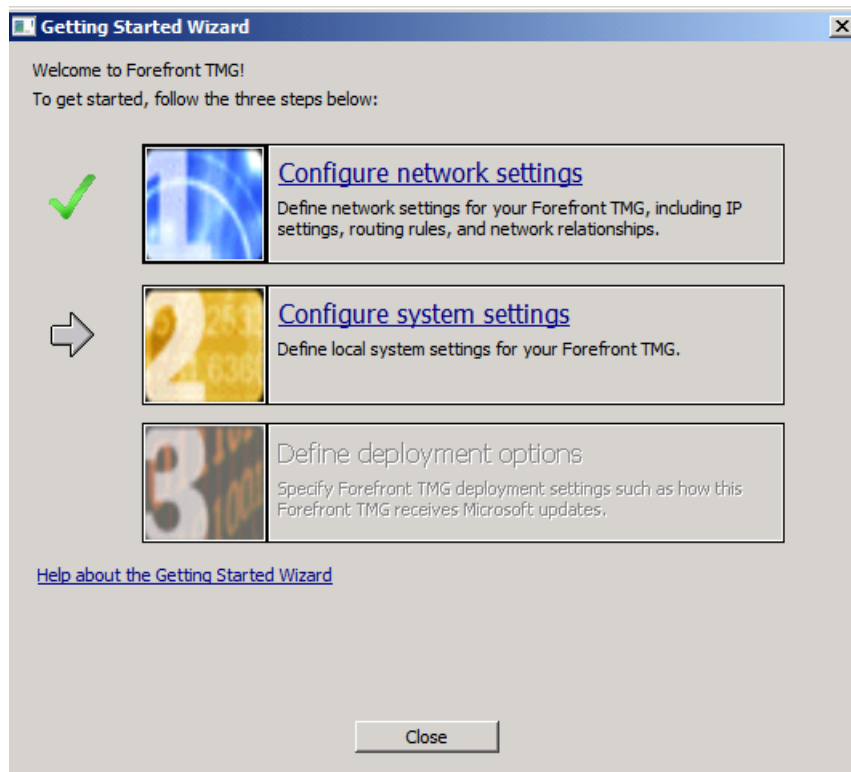
Network adapter connected to the LAN:  
Local Area Connection

☐ Obtain an IP address automatically  
☒ Use the following IP address

IP address: 192 . 9 . 200 . 121  
Subnet mask: 255 . 255 . 255 . 0  
Default gateway: . . .  
DNS server: . . .

 If a dynamic IP address is used (DHCP), clients on the Internal network must either have their Web browsers configured to use Forefront TMG as their Web proxy or should be running the Firewall Client software.

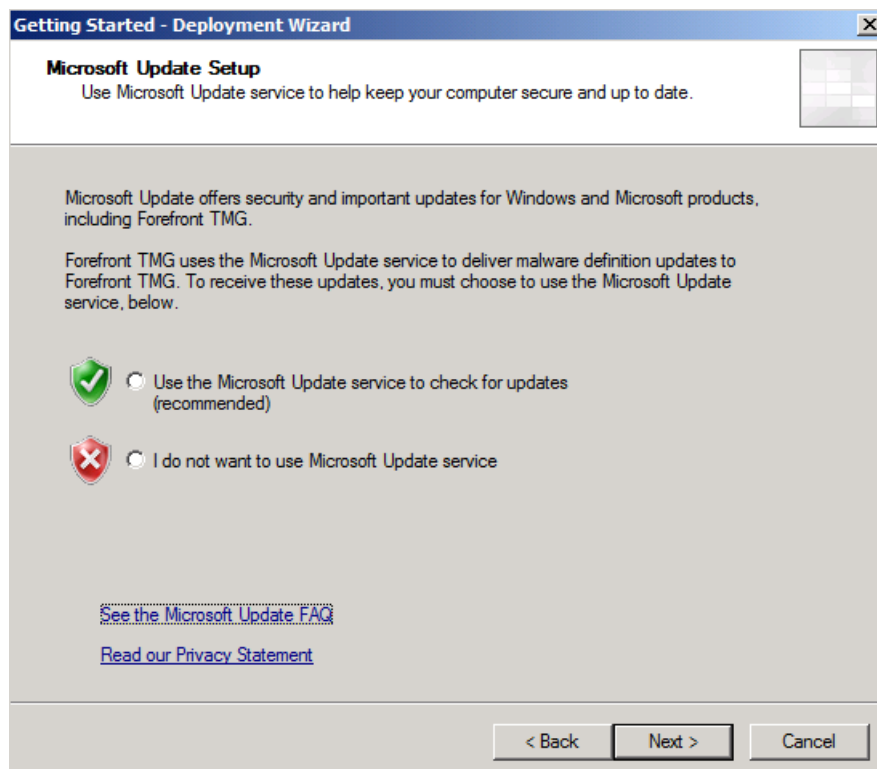
< Back   Next >   Cancel







Ein grosser Schwerpunkt in diesem Build sind die integrierten Maleware Defintion Updates.



**Getting Started - Deployment Wizard**

**Definition Update Settings**  
Select how definition updates will be downloaded and installed on this system.


Automatic Update Action

Malware inspection: Check and install

Automatic Update Action Polling Frequency

☒ Every 15 minutes

☐ Everyday at 3:00 AM

 Requesting definition updates from Microsoft requires you to have a subscription license.

< Back Next > Cancel

**Getting Started - Deployment Wizard**

**Customer Feedback**  
We invite you to join the Customer Experience Improvement Program to help us improve the quality, reliability and performance of this product.

This program collects anonymous information about your hardware configuration and how you use this product, without interrupting you. We use the information to identify trends and usage patterns. No information is used to identify or contact you.

If you participate in the program, Web proxy client access will be enabled on the Forefront TMG Local Host network.

You can change your participation choice after closing this dialog box. To do this, open the server or array property pages, and modify settings on the Customer Feedback tab.

[Learn more about the Customer Experience Improvement Program](#)

☒ Yes, I am willing to participate anonymously in the Customer Experience Improvement Program (recommended)

☐ No, I don't wish to participate

< Back Next > Cancel

Microsoft Telemetry Service

Getting Started - Deployment Wizard

Microsoft Telemetry Service

Select a telemetry membership option.

Microsoft Telemetry Service helps protect against malware and intrusion by reporting information to Microsoft about potential attacks, which Microsoft uses to help identify attack patterns and improve precision and efficiency of threat mitigations. In some instances, personal information might be inadvertently sent to Microsoft, but Microsoft will not use this information to identify or contact you.

Select your Microsoft Telemetry Service membership type:

☐ Join with a basic membership

Forefront TMG will report basic information about potential threats identified, including threat type, where it originated, and the action applied.

☒ Join with an advanced membership

In addition to basic information, Forefront TMG will report additional details about potential threats, including traffic samples and full URL strings. With advanced membership, you provide Microsoft with more help in analyzing and mitigating threats.

☐ I do not want to join Microsoft Telemetry Service at this time. Do not send any information to Microsoft.

[Read our Privacy Statement](#)

< Back

Next >

Cancel

Web Access Policy Wizard

Microsoft  
Forefront  
Threat Management Gateway

This wizard helps you define how internal users access the Internet, the types of Web sites they are allowed to access, malware inspection settings, and if content downloaded from the Internet is stored in the cache.

When you complete this wizard, access policy rules for the applied settings will be created.

To continue, click Next.

Welcome to the Web Access Policy Wizard

< Back

Next >

Cancel

**Web Access Policy Wizard** [X]

**Web Protection**

A valid license is required to use the malware inspection feature.

Do you want to use the malware inspection feature for HTTP traffic?

☒ Yes, enable the malware inspection feature

☐ No, do not enable the malware inspection feature

Malware inspection is available for evaluation without a license for 90 days following installation. When the evaluation period ends, you will need to purchase a valid license.

[Help about purchasing a valid HTTP protection license](#)

< Back   Next >   Cancel

**Web Access Policy Wizard** [X]

**Web Access Policy Type**


You can apply a single policy to all the clients in your organization or specify different policies based on users or computers.

☐ Create a simple Web access policy for all the clients in my organization

This policy allows clients in your organization access to all Web sites and destinations except those that you explicitly block. Only choose this option if internal users are not required to authenticate for Internet access.

☒ Create customized Web access policies for users, groups and computers

This option allows you to apply allow and deny policies for different users, groups or computers in your organization. Choose this option if you require some or all users in your organization to authenticate for Internet access.

 Forefront TMG is currently not joined to a Microsoft domain. Using the Web Access Wizard to create a customized policy for authenticated users is only supported when Forefront TMG is a domain member.

< Back   Next >   Cancel

**Web Access Policy Wizard** [X]

**Default Web Access Policy**  
Select how Web access attempts that do not match any settings defined in the Web access policy will be handled.

Action applied when a Web request is not explicitly allowed or denied by Web access policy:

☒ Allow the Web request


☐ Deny the Web request

< Back   Next >   Cancel

**Add Access Policy** [X]

Policy Name:

Access Groups:


 Internal

Add... Edit... Remove

☒ Allow access to the destinations below

☐ Deny access to the destinations below

Destinations:

 External

Add... Edit... Remove

OK Cancel

**Web Access Policy Wizard** [X]

**Anonymous Web Access Policies**  
Define how Web requests not requiring authentication are handled (allowed or denied).

Anonymous Web access policies:

Access Groups	Destinations
✓ Internal	External

Buttons: Add... Edit... Remove ↓ ↑

Policy Name: Test UTM

< Back Next > Cancel

**Web Access Policy Wizard** [X]


**Malware Inspection Setting**  
With malware inspection enabled, HTTP content requested from the Internet can be scanned for malware, such as viruses and spyware.

The malware inspection feature is enabled. Select if you want to apply malware inspection to the rules created by the Web Access Policy Wizard.

☐ Do not inspect Web content requested from the Internet  
☒ Inspect Web content requested from the Internet

☒ Allow partial file delivery  
 Forefront TMG will send content to clients as it is inspected, rather than wait for the entire scan to complete. This results in a better user experience.

☒ Block encrypted archives (for example, zip files)  
 Forefront TMG will block the downloading of all encrypted archive files. Such files may contain encrypted viruses capable of bypassing antivirus signatures.

 This option applies only to rules created by the Web Access Policy Wizard. To enable malware inspection on other rules, you must enable malware inspection in the rule properties.

< Back Next > Cancel

**Web Access Policy Wizard**

**Web Cache Configuration**  
 With Web caching enabled, frequently accessed Web content is stored in the cache, improving browser performance and reducing bandwidth consumption.

☒ Enable Web caching

Assign the cache drives and drive space used for Web caching:

Server	Cache Size (all disks)	Free Space (all disks)
WIN-UBF8P1T5DHX	50 MB	118432 MB

[Cache Drives...](#)

With Web caching enabled, a cache rule enabling the caching of Web content requested from the Internet (External network) will be created.  
[Help about Web caching](#)

< Back    Next >    Cancel

**Forefront TMG**

File Action View Help

Microsoft Forefront Threat Management Gateway

Microsoft Forefront Threat Management Gateway

**All Firewall Policy**

Order	Name	Action	Protocols	From / Listener	To	Condition	Description	Policy
<b>Web Access Policy Group</b>								
1	Web Access Ano...	Allow	HTTP HTTPS	Internal	External	All Users	Web access rule ...	Array
2	Web Access Defa...	Allow	HTTP HTTPS	Internal	External	All Users	Web access rule ...	Array
Last	Default rule	Deny	All Traffic	All Networks (...)	All Networks (...)	All Users	Predefined acces...	Array

Microsoft Forefront Threat Management Gateway

Monitoring Forefront TMG (WIN-UBF8P1TSDH)

File Action View Help

Microsoft Forefront Threat Management Gateway

Monitoring Forefront TMG (WIN-UBF8P1TSDH)

Dashboard Alerts Sessions Services Configuration Reporting Connectivity Verifiers Logging

Tasks Help

Refresh

Refresh Now

Automatic Refresh Rate

Medium

Connectivity Verifiers

Group Type	Status
Active Directory	Not Configured
DHCP	Not Configured
DNS	Not Configured
Others	Not Configured
Published Ser...	Not Configured
Web (Internet)	Not Configured

Services

Service	Status	Servers Up
Firewall	Started	1 out of 1
Job Scheduler	Started	1 out of 1
SQL Server E...	Started	1 out of 1

Alerts

Latest	Alert	Severity	New	Server
4/9/2008 ...	Accumulation Fol...	Information	1	WIN-UBF8P1T
4/9/2008 ...	Microsoft Update ...	Warning	1	WIN-UBF8P1T
4/9/2008 ...	Definition Update...	Error	1	WIN-UBF8P1T
4/9/2008 ...	Service Shutdown	Information	1	WIN-UBF8P1T
4/9/2008 ...	Malware Inspecti...	Information	2	WIN-UBF8P1T
4/9/2008 ...	Malware Inspecti...	Warning	2	WIN-UBF8P1T
4/9/2008 ...	Service Started	Information	4	WIN-UBF8P1T
4/9/2008 ...	Definition Updatin...	Error	4	WIN-UBF8P1T

Sessions

Server	Total	Web Proxy	Firewall Client	SecureNAT
WIN-UBF8P1...	5	2	0	3

Update Services

Service	Status
Malware Inspection	In Progress

Configuration Storage Server wie bei ISA 2006 Enterprise, im Detail aber doch ganz anders

Microsoft Forefront Threat Management Gateway

Monitoring Forefront TMG (WIN-UBF8P1TSDH)

File Action View Help

Microsoft Forefront Threat Management Gateway

Monitoring Forefront TMG (WIN-UBF8P1TSDH)

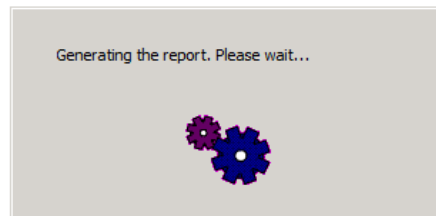
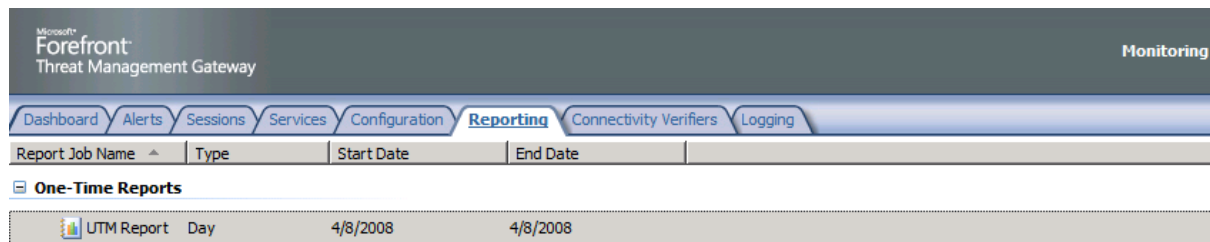
Dashboard Alerts Sessions Services Configuration Reporting Connectivity Verifiers Logging

Configuration Status

Configuration status monitors the version of the configuration used by the Microsoft Firewall Service on each array member and compares it to the version of the configuration stored in ADAM.

Server	Status	Last Updated	Description
WIN-UBF8P1...	Synced	4/9/2008 8:53:10 PM	Server configuration matches the Configuration Storage se...

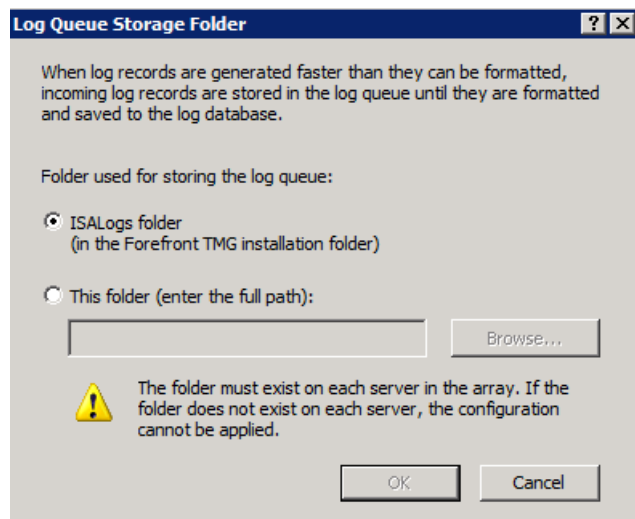




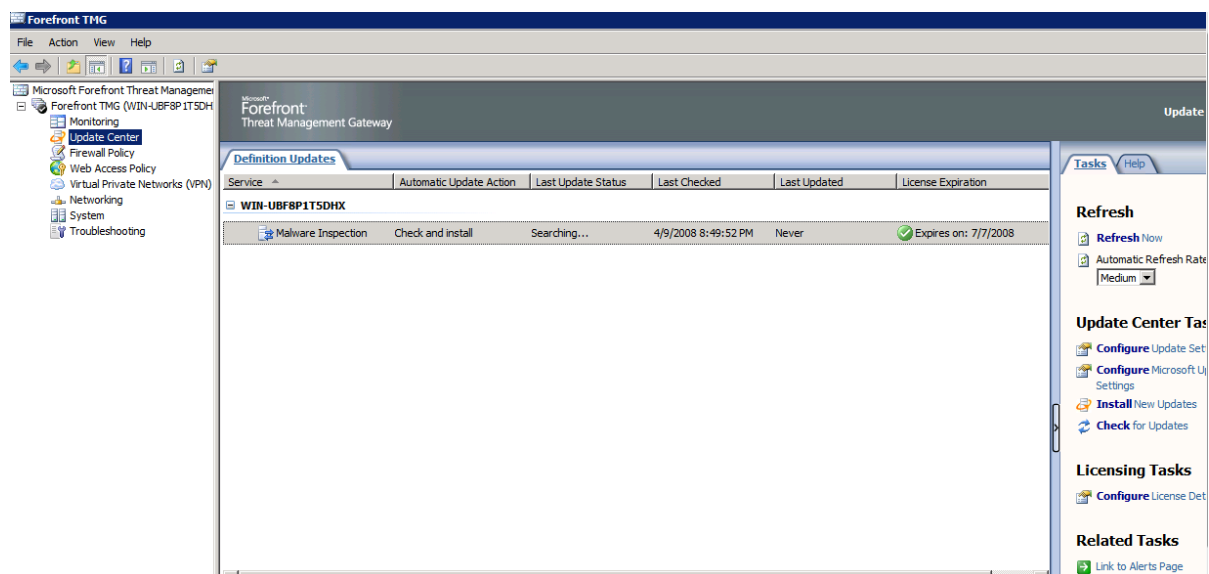
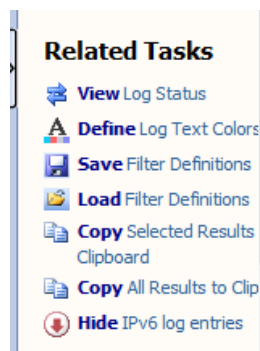
Der Report – noch etwas leer, da kein Traffic



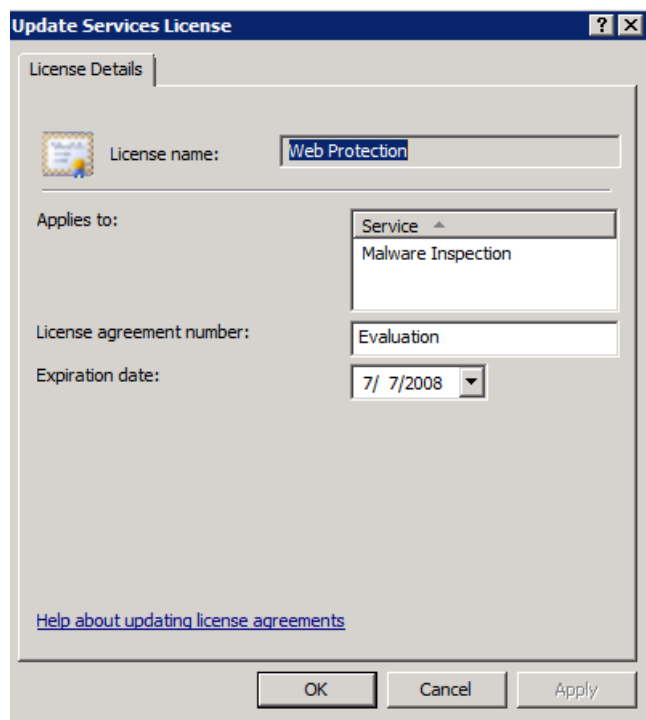
Neu: Log Queue Storage Folder



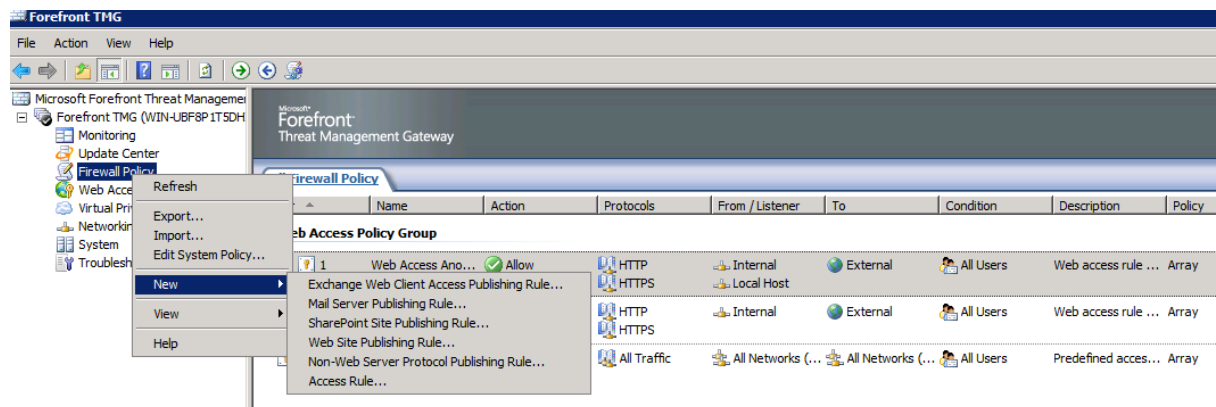
Ah, IPv6



Update Services Lizenz



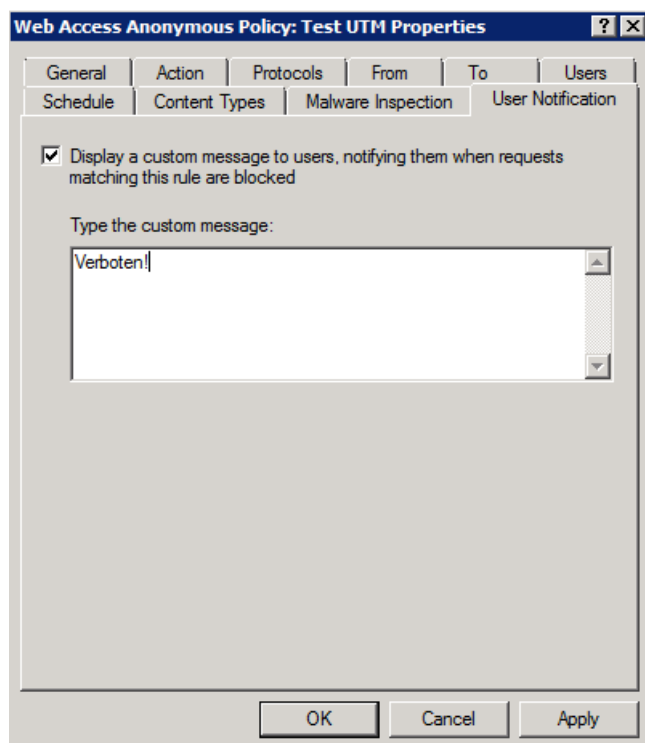
## Firewall Regeln



## Ein paar neue Registerkarten



Cool: Custom Text bei verbotenen Seiten:



HTTP Filter ist unverändert geblieben

**Configure HTTP policy for rule** [?] [X]

General | Methods | Extensions | Headers | Signatures

**Request Headers**  
Maximum headers length (bytes):

**Request Payload**  
☒ Allow any payload length  
Maximum payload length (bytes):

**URL Protection**  
Maximum URL length (bytes):   
Maximum query length (bytes):   
☐ Verify normalization  
☐ Block high bit characters

**Executables**  
☐ Block responses containing Windows executable content

OK Cancel Apply

## Schwerpunkt Webzugriff

Microsoft  
**Forefront**  
Threat Management Gateway

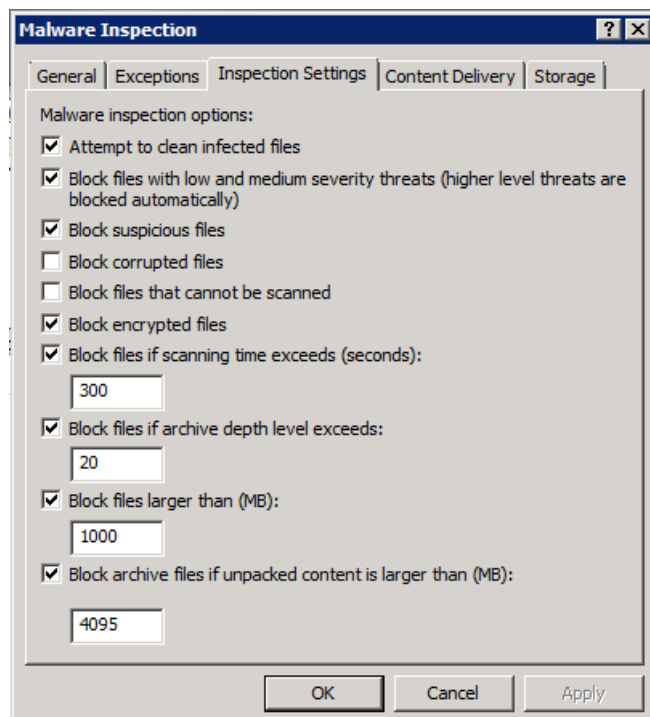
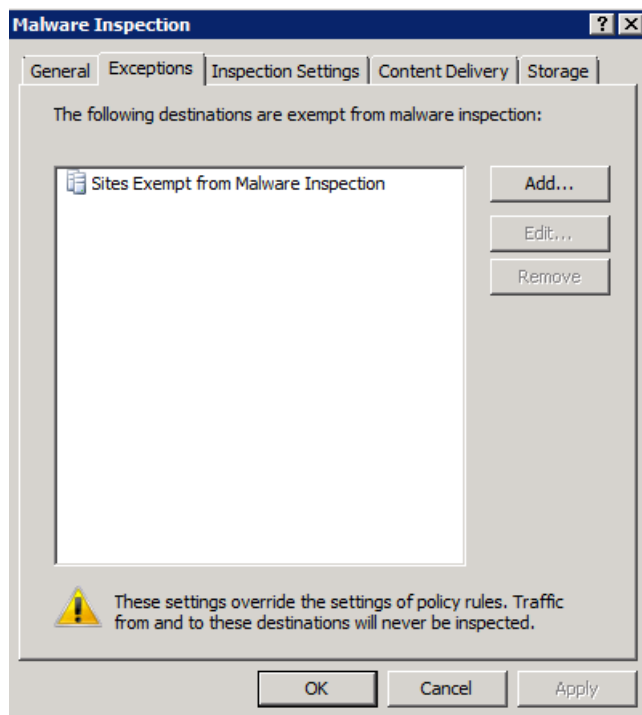
**Web Access Policy**

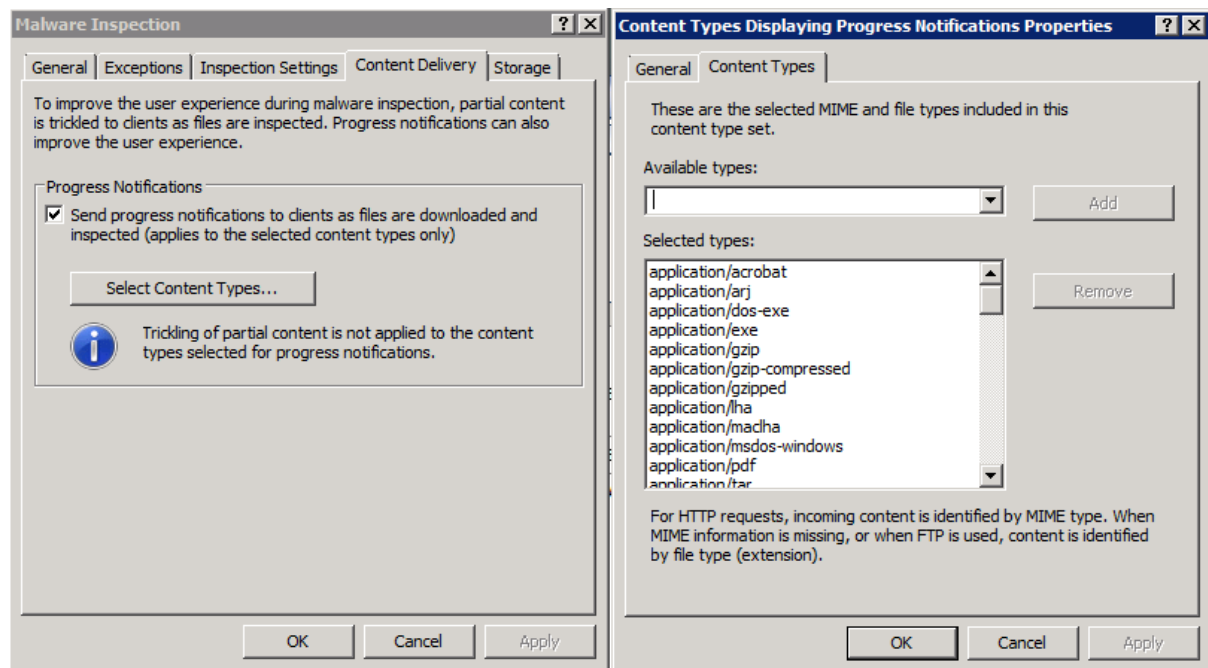
Web Access Settings

Web Proxy: Enabled (Port: 8080)      Malware Inspection: Enabled  
Authentication: Not required by policy      Web Caching: Enabled  
HTTP Compression: Enabled

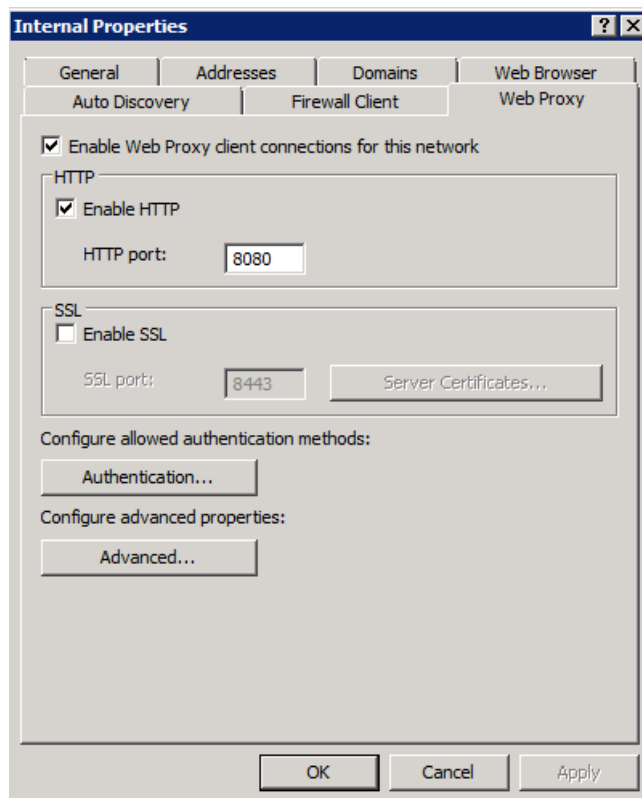
Action	Name	Condition	From	To
<b>Web Access Policy Group</b>				
Deny	Web Access ...	All Users	Internal Local Host	External
Allow	Web Access ...	All Users	Internal	External
Deny	Default rule	All Users	All Networks (...)	All Networks (...)

## Malware Inspection

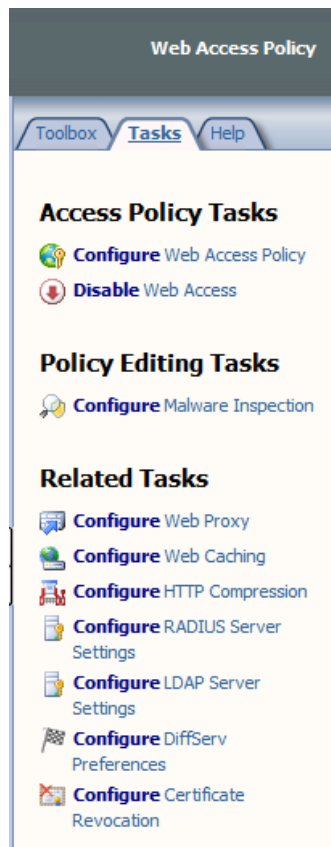




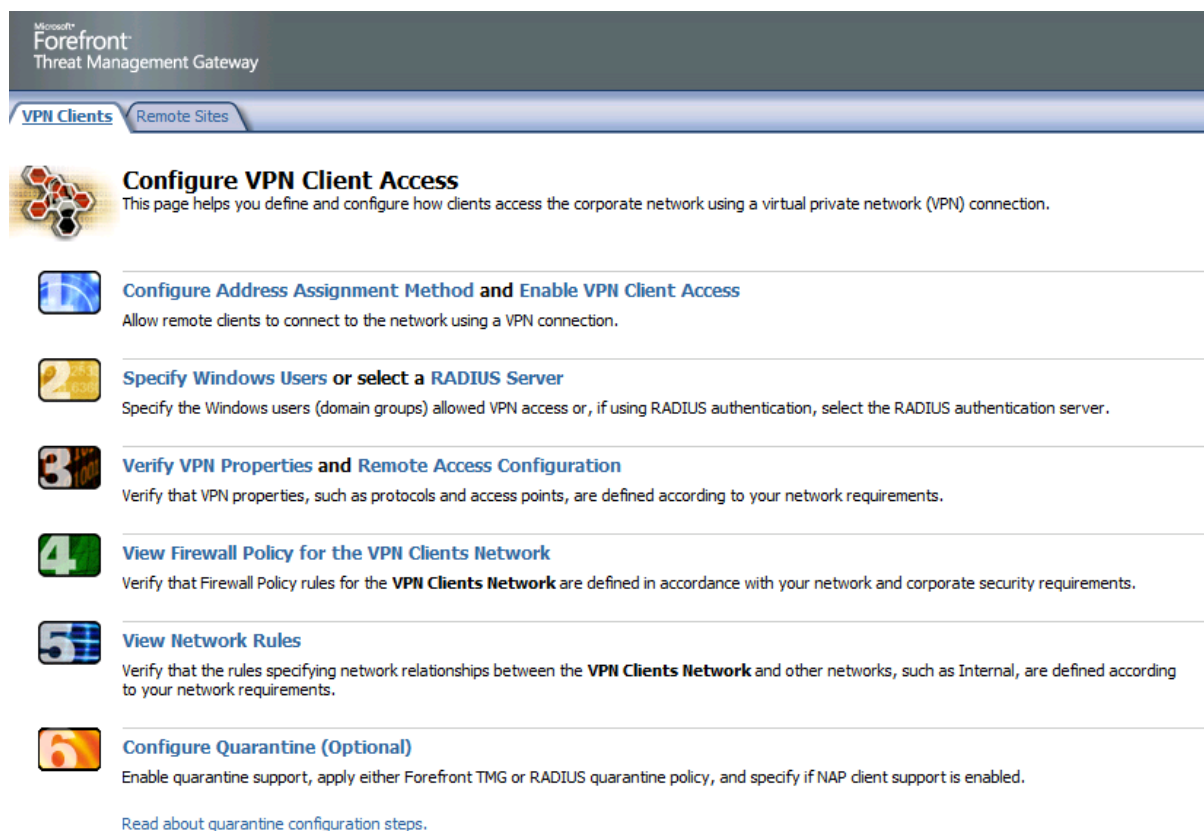
Webproxy – Im ISA nix neues



Auch hier auf dem ersten Blick nichts Neues:



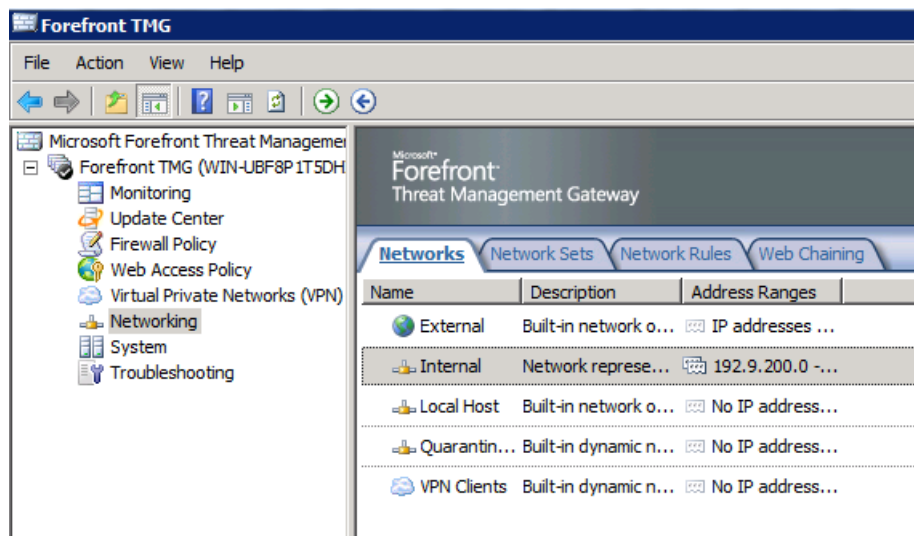
1 – 2 – 3 – 4 – 5 – 6 – einer mehr als bei ISA 2006 (und doch nicht wirklich)



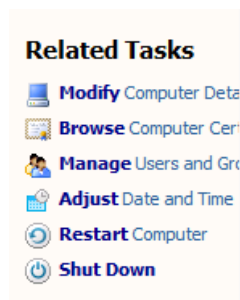
Im VPN Bereich sonst auf dem ersten Blick wenig neues (kein SSTP, IAG Anteil etc).



Netzwerkbereich – Hier auch alles unverändert?!



Ein paar Tools mehr in der Konsole



Neue(r) Filter

Microsoft Forefront Threat Management Gateway			
Servers Application Filters Web Filters			
Name	Description	Vendor	Version
DNS Filter	Filters DNS traffic	Microsoft (R) Cor...	4.0
FTP Access Filter	Enables FTP prot...	Microsoft (R) Cor...	4.0
H.323 Filter	Enables H.323 pr...	Microsoft (R) Cor...	4.0
MMS Filter	Enables Microsoft...	Microsoft (R) Cor...	4.0
PNM Filter	Enables RealNet...	Microsoft (R) Cor...	4.0
POP Intrusion Detection Filter	Checks for POP b...	Microsoft (R) Cor...	4.0
PPTP Filter	Enables PPTP tun...	Microsoft (R) Cor...	4.0
RPC Filter	Enables publishin...	Microsoft (R) Cor...	4.0
RTSP Filter	Enables Real Tim...	Microsoft (R) Cor...	4.0
SMTP Filter	Filters SMTP traffic	Microsoft (R) Cor...	4.0
SOCKS V4 Filter	Enables SOCKS 4 ...	Microsoft (R) Cor...	4.0
TFTP Access Filter	Enables TFTP pro...	Microsoft (R) Cor...	4.0
Web Proxy Filter	Enables HTTP pro...	Microsoft (R) Cor...	4.0

Wo ist denn der SIP Filter geblieben? Der war doch schon mal da?

Microsoft Forefront Threat Management Gateway						
Servers Application Filters Web Filters						
Order	Name	Description	Version	Vendor	Relative Path	Direction
1	DiffServ Filter	Enables DiffServ ...	4.0	Microsoft (R) Cor...	DiffServ.dll	Both
2	Web Publishing Load Balancing Filter	Enables publishin...	4.0	Microsoft (R) Cor...	WPLoadBalancer.dll	Incoming Web R
3	Compression Filter	Enables HTTP/HT...	4.0	Microsoft (R) Cor...	comphp.dll	Both
4	Authentication Delegation Filter	Enables authentic...	4.0	Microsoft (R) Cor...	authdflt.dll	Incoming Web R
5	Forms-Based Authentication Filter	Enables forms-ba...	4.0	Microsoft (R) Cor...	CookieAuthFilter.dll	Incoming Web R
6	RADIUS Authentication Filter	Enables RADIUS ...	4.0	Microsoft (R) Cor...	radiusauth.dll	Both
7	LDAP Authentication Filter	Provides LDAP Au...	4.0	Microsoft (R) Cor...	ldapfilter.dll	Incoming Web R
8	Link Translation Filter	Enables link transl...	4.0	Microsoft (R) Cor...	LinkTranslation.dll	Incoming Web R
9	Malware Inspection Filter	Enables inspectio...	4.0	Microsoft (R) Cor...	EmpFilter.dll	Outgoing Web R
10	HTTP Filter	Filters HTTP traffi...	4.0	Microsoft (R) Cor...	HttpFilter.dll	Both
11	Caching Compressed Content Filter	Enables caching o...	4.0	Microsoft (R) Cor...	complp.dll	Both

Neue Namen – gleiche Inhalte

Microsoft

Forefront

Threat Management Gateway

Troubleshooting

## Troubleshooting and Support

### Use the ISA Server Best Practices Analyzer

The ISA Server Best Practices Analyzer Tool scans the configuration settings of the local Forefront TMG computer, determining the status of the Forefront TMG computer configuration and finding issues that do not conform to recommended best practices.

### View Forefront TMG Alerts

Forefront TMG alerts notify you when specified events occur on the local Forefront TMG computer. Click this link to open the Alerts tab in the Forefront TMG Monitoring options.

### View Forefront TMG Logging

Forefront TMG maintains logs of activity on the Forefront TMG computer. Click this link to open the Logging tab in the Forefront TMG Monitoring options.

### Read Forefront TMG Documentation

Learn more about Forefront TMG.

## Microsoft Forefront TMG Performance Monitor

